ROBERT S. SHWARTS (STATE BAR NO. 196803)
rshwarts@orrick.com
CATHERINE Y. LUI (STATE BAR NO. 239648)
clui@orrick.com
NATHAN SHAFFER (STATE BAR NO. 282015) nshaffer@orrick.com
JOHANNA L. JACOB (STATE BAR NO. 286796)
jjacob@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
The Orrick Building
405 Howard Street
San Francisco, CA 94105-2669
Telephone: +1 415 773 5700
Facsimile: +1 415 773 5759

Attorneys for Plaintiff
ExamWorks, LLC

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

EXAMWORKS, a Delaware limited liability company, Plaintiff, v. TODD BALDINI, an individual, ABYGAIL BIRD, an individual, LAWRENCE STUART GIRARD, an individual, PAMELLA TEJADA, an individual, ROE CORPORATION, and DOES 1 through 10, Defendant(s).	No. 2:20-cv-00920-KJM-DB STIPULATED ORDER RE: DISCOVERY OF ELECTRONICALLY STORED INFORMATION FOR STANDARD LITIGATION

1. PURPOSE

This production protocol will govern how the parties and the stipulated third party neutral forensic examiner produce email and electronic documents in this action.

2. SEARCH OBLIGATIONS

a. Each Party will conduct a reasonably diligent search for accessible sources of Electronically Stored Information ("ESI") in which it has reason to believe potentially relevant material will be found.

b. Furthermore, each Party represents that, from the point of its own reasonable anticipation of litigation, it has taken reasonable steps to prevent the partial or full destruction, alteration, shredding, incineration, wiping or loss, due to any reason whatsoever, of potentially relevant information contained in hard copy or reasonably accessible sources of ESI.

3. DOCUMENT PRODUCTION FORMAT

a. TIFF Images. Unless otherwise stated in this Production Protocol, each document shall be produced in black and white, CCITT Group IV Tagged Image File Format ("TIFF") regardless of whether such documents are stored by the parties in the ordinary course of business in electronic or hard copy form. Each TIFF image file should be one page and should reflect how the source document would appear if printed to hard copy.

b. Load File(s). Document productions shall include Concordance-compatible Load File(s) that indicates document breaks of the TIFF images and additional fields as identified in Section 6 below.

c. File Name. Each document image file shall be named with the unique Bates Number of the first page of the document in question followed by the file extension "TIF". File names should not be more than fifteen characters long or contain spaces or underscore symbols.

d. Document Unitization. Electronically collected data shall maintain family relationships to group parent documents with their attachments. Parties shall apply all appropriate measures to logically unitize any hard copy or scanned documents in order to represent how they were maintained in the ordinary course of business.

e. Color. Documents shall be produced as black and white TIFF images. Upon written request, a party shall produce color images for a reasonable number of selected documents. Documents produced in color shall be produced as JPEG images with Exif compression and 24-bit color depth. Each color document image file shall be named with the unique Bates Number of the first page of the document in question followed by the file extension "JPG".

f. Confidentiality Designation. Responsive documents in TIFF format will be stamped with the appropriate confidentiality designations in accordance with the Protective Order in this matter. Each responsive document produced in native format will have its confidentiality designation identified in the filename of the native file.

g. Native Production for Spreadsheets, PowerPoint Presentations, and other Files not readily converted into TIFF images. Notwithstanding the foregoing, the parties will produce spreadsheet and PowerPoint and other presentation files in native format, as well as any other files not readily converted into a TIFF image (e.g., audio or video files). Each file produced in native format shall be named with a unique Bates Number (*e.g.*, ABC00000001.xls) and protective designation (*e.g.* ABC00000001_confidential.xls). In addition to producing such documents in native format, the producing party shall also include in the production a placeholder TIFF image with the phrase "Document Produced Natively." The placeholder TIFF images shall be Bates-numbered as described herein, shall be endorsed for confidentiality as described in the Protective Order, and shall include

Metadata as set forth in Section 4. The parties reserve the ability to request other file types be produced in native form or in another reasonably usable form upon review of the other party's production. The parties reserve their respective rights to object to any such request

h. Native Redactions. Spreadsheets that contain redactions shall be produced as TIFF images, and shall follow the TIFF-image protocol described herein. However, when reasonably necessary, large spreadsheets that contain redactions may be produced in native format with black boxes representing the redacted portions of the document. These documents shall be redacted using a "full block" representative character that appears as a black box on the spreadsheet. This process may be used when a TIFF image would otherwise result in a large number of pages such that it is unreasonable to review as a TIFF image.

4. **SEARCHABLE TEXT.** In addition to TIFF images, each production will include text files corresponding to the TIFF image files described above.

a. Hard Copy Documents. Hard copy documents shall be scanned using Optical Character Recognition ("OCR") technology and searchable ASCII text (or Unicode text if the text is in a language requiring characters outside of the ASCII character set) files shall be produced. Each file shall be named with the unique Bates Number of the first page of the corresponding TIFF document followed by the extension "TXT". Hard copy documents shall otherwise be produced as they are stored in the normal course of the producing party's business.

b. Electronic Documents. The full text of each native electronic document shall be extracted ("Extracted Text") and produced in a text file. The Extracted Text shall be provided in searchable ASCII text format (or Unicode text format if the text is in a language requiring characters outside of the ASCII character set) and shall be named with the unique Bates Number of the first page of the corresponding TIFF document followed by the extension "TXT". Searchable text files corresponding to the TIFF image files for redacted Electronic Documents must include Extracted Text or OCR text only to the extent that it will not disclose redacted information.

5. **PRODUCTION MEDIA**

a. Documents that are designated pursuant to the protective order must be produced via encrypted media or via encrypted FTP transfer or other securely encrypted electronic transmissions. Such productions must also be password protected, with the passcode being securely and separately transferred from the encrypted media itself. Non-designated documents may be included in the encrypted production of designated documents, but a production of exclusively non-designated documents may be produced without encryption. The encryption passcode for any encrypted media will be exchanged between counsel for the parties securely and separately transferred from the encrypted media itself. Encryption passcodes may only be disclosed to parties, parties' counsel, experts, third-party vendors, and support staff for all of these entities. The encryption specification used will be the Advanced Encryption Standard ("AES") established by the U.S. National Institute of Standards and Technology and will use a 256 bit key length. Passcodes must be at least 14 characters long and contain a mix of upper case characters, lower case characters, numbers, and symbols such as "&" or "$" or others and will not contain any complete words. Each FTP production transfer and piece of Production Media shall identify: (1) the producing party's name; (2) the production date; and (3) the Bates Number range of the materials contained on the Production Media.

6. **METADATA**

a. For all Electronic Documents, the Concordance compatible Load File(s) referenced in paragraph 3(b) will be in an ASCII text format and include the Data Fields listed below. For redacted Electronic Documents, metadata fields must be produced only to the extent such fields will not disclose redacted information.

b. The parties reserve the ability to request that additional Data Fields be set forth or provided for certain specified Electronic Documents upon review of the other party's production. A party is not obligated to produce metadata from a document if metadata does not exist in the document, or if the metadata is not machine-extractable. Notwithstanding, the Custodian and Hash Value fields identified in Appendix A are derived or additive metadata which the parties must produce even though not otherwise existing in the document or machine-extractable.

Field	**Field Name**	**Field Format**	**Description**
Confidentiality	Confid	Text	Confidentiality designation pursuant to the parties' Protective Order
File Name	FileName	Text	File Name of document or email
File Size	FileSize	Text	File size of document or email (including any embedded attachments)
Document Page Count	PageCount	Non zero filled number	Number of pages in email or document
Production Begin Bates Number	BegDoc	Maximum six-character alpha prefix, seven-digit numeric sequence	Document ID number associated with first page of email or document
Production End Bates Number	EndDoc	Maximum six-character alpha prefix, seven-digit numeric sequence	Document ID Number associated with last page of email or document
Production Begin Attachment Bates Number	BegAtta	Maximum six-character alpha prefix, seven-digit numeric sequence	Document ID Number associated with first page of parent email, document or family
Production End Attachment Bates Number	EndAtta	Maximum six-character alpha prefix, seven-digit numeric sequence	Document ID Number associated with last page of email, document or family
Parent ID	ParentID	Maximum six-character alpha prefix, seven-digit numeric sequence	Starting Bates number of Parent document

Attach IDs	AttachIDs	Maximum six-character alpha prefix, seven-digit numeric sequence	Starting Bates number of each attached document separated by semi-colon
Attach Count	Attachcount	Number	Tally of the number of attachments per document
Document Type	DocType	Text	Type of document (e.g., email, attachment, network document)
Original File Path	OrigPath	Text	Complete original file path for an email or loose electronic document
Duplicate Path	DupPath	Text	Only applicable when loose files are de-duplicated against email attachments
Application	AppName	Text	Type of application of document or email (*i.e.*, Outlook, Lotus Notes, Microsoft Word or Microsoft Excel, etc.)
File Extension	FileExt	Text	File extension of document or email
Full Text Path	TextPath	Text	UNC path to production text files containing the extracted or OCR text (Not required if text of document is redacted)
MD5/SHA1	MD5Hash/ Secure Hash	Hash value	Algorithm that represents a unique value of the document or email, used for deduplication purposes
Native Link	Native Link	Text	Complete file path of produced native file to allow hyperlinking of native file. (Only if native file is being produced)
Redacted Document	RedctDoc	Y/N	If a document is redacted, this field must contain a "Y." If the document has not been redacted, the field must contain an "N."
Custodian	DocCust	Text	Name of the custodian or source system from which the document was collected.

Duplicate Custodian[1]	DupCust	Text semicolon delimited	List of custodian names that had duplicates of this email or document. Names shall be delimited by a semicolon. Only applicable when the parties use global deduplication.
Author	Author	Text	Document author name, for non-email documents.
Last Author	LastAuthor	Text	Last author or editor of document, from document properties
From	Sender	Text	Name and/or email address of person(s) found in the "FROM" address line.
To	Recipient	Text semicolon delimited	Name(s) and/or email addresses of person found in the "TO" address line.
CC	CC	Text semicolon delimited	Name(s) and/or email addresses of person(s) found in the "CC" address line.
BCC	BCC	Text semicolon delimited	Name(s) and/or email addresses of person(s) found in the "BCC" address line, if any.
Subject	Subject	Text	Subject or "Re" line of email; not required for documents if subject or re line is redacted.
Title	Title	Text	Title of non-email document; not required if title is redacted.
Date Created	CreateDate	Date in MMDDYYYY	Date on which the document was created
Time Created	CreateTime		Time file created
Last Modified Date	DateMod	Date in MMDDYYYY	Date the document was last modified
Last Modified Time	ModTime		Time file last modified
Last Access Date	AccessDate	Date in MMDDYYYY	Date file last accessed
Last Access Time	AccessTime		Time file last accessed

[1] Global Deduplication is the recommended processing standard for most matters. The Parties shall attempt to de-duplicate ESI to avoid substantially duplicative productions. Documents will be de-duplicated against the entire population and all custodians of a de-duplicated document will be listed in a "Duplicate Custodian" field.

Sent Date	DateSent	Date in MMDDYYYY	Date email was sent
Sent Time	TimeSent		Time email was sent
Date Received	DateRecd	Date in MMDDYYYY	Date email was received by addressed recipients
Time Received	TimeRecd		Time email was received
Drive ID	DriveID	Text	Serial number or ID of external hard drive or thumb drive that document originates from.

7. EMAIL THREADING

a. In order to reduce the volume of entirely duplicative content within email threads, a party may utilize email thread suppression. As used in this agreement, email thread suppression means reducing redundant production of lesser inclusive email threads by producing the most recent email containing the thread of emails, as well as any emails with unique attachments within the thread. Thus excluding all lesser inclusive emails that would constitute redundant duplicates within the produced string. Emails suppressed under this paragraph need not be reflected on the party’s privilege log.

8. TIMEZONE

a. All documents and associated metadata shall be produced in the UTC time zone.

9. EXTERNAL HARD DRIVES AND USB DRIVES

a. The parties will produce both files and folders from external hard drives and USB Drives, including Metadata as set forth in Section 6. In addition, files and folders produced from external drives and USB Drives must be produced with the embedded or internal serial number of the source drive (see field above called DriveID).

10. PRIVILEGE LOGS

a. For each document withheld on the basis of privilege, the parties agree to include such document on a furnished log that complies with the legal requirements under federal law, but at a minimum will include the following information:

i. A unique number for each entry on the log.

ii. The date of document. The parties should indicate what the date of the document signifies. For example, this could be the sent date of the document or the last-modified or create date of the document.

iii. The Author of the document. For emails this should be populated with the metadata extracted from the "Email From" field associated with the file. For loose ESI, this should be populated with the metadata extracted from the "Author" field; if such field contains generic information such as the company name, a party may substitute the information contained in the "Custodian" metadata field.

iv. Recipient(s) of the document where reasonably ascertainable. For emails this should be populated with the metadata extracted from the "Email To" field associated with the file. Separate columns should be included for the metadata extracted from the "Email CC" and "Email BCC" fields, where populated.

v. A description of why privilege is being asserted over the document. This description should include information sufficient to identify if the document contained attachments over which privilege is also being asserted.

vi. The type of privilege being asserted: (a) AC for Attorney/Client, (b) WP for Attorney Work Product, (c) CI for Common Interest.

vii. The parties shall identify on their logs the counsel who is the basis of the privilege or work product claim where not otherwise apparent from the identifying information.

IT IS SO STIPULATED, through Counsel of Record.

Dated: June 9, 2020 *-/s/ Catherine Y. Lui*

Counsel for Plaintiff ExamWorks, LLC

Dated: June 5, 2020 */s/ Daniel Benjamin Chammas*

Counsel for Defendants Todd Baldini, Stuart Girard,
Pamella Tejada, and Abygail Bird

ORDER

Pursuant to the parties' stipulation, IT IS SO ORDERED.

DATED: June 11, 2020

/s/ DEBORAH BARNES
UNITED STATES MAGISTRATE JUDGE